

Appl. No. 09/489,696  
Amdt. Dated July 12, 2004  
Reply to Office Action of February 12, 2004

Attorney Docket No. 81800.0018  
Customer No.: 26021

### **REMARKS/ARGUMENTS**

In response to the Office Action dated March 6, 2003, claims 3, 4, 8, 15, 15, 19, 22, and 23 are amended, and claims 1, 2, and 10-12 are canceled without prejudice, waiver, or disclaimer to the subject matter contained therein. Claims 3-9 and 13-23 remain in the application. It is not the Applicants' intent to surrender any equivalents because of the amendments or arguments made herein. Reexamination and reconsideration of the application, as amended, are respectfully requested.

#### **Art-Based Rejections**

In paragraphs 1-2 of the Office Action, claims 1-4, 7-13, and 22 were rejected under 35 U.S.C. § 102(e) as being anticipated by Baba, USPN 5,987,129.

In paragraphs 3-4 of the Office Action, claims 5-6, 14-21, and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Baba, USPN 5,987,129.

The Applicant respectfully traverses the rejections, however, in order to expedite prosecution, the Applicants have amended the claims. The Applicants respectfully submit that the claims are patentable in light of the amendments above and the arguments below.

#### **The Baba Reference**

The Baba reference discloses a method of sharing a cryptokey. To achieve the above object, there is provided in accordance with a first aspect of the present invention a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of

entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities. See Col. 2, lines 45-63.

The Claims are Patentable over the Cited Reference

The claims of the present invention describe cryptographic communications methods. A method in accordance with the present invention, for communications of information between entities wherein a plurality of centers are provided, comprises each of the centers generating secret keys peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities; one entity generates a first common key using a first component contained in at least one secret generated by at least one of the plurality of centers, the secret key being peculiar to the one entity, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts said

ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity.

The cited reference does not teach nor suggest the limitations of the claims of the present invention. Specifically, the cited references does not teach nor suggest at least the limitation of each of the centers generating secret keys using divided pieces of information specifying each of the entities where one entity generates a first common key using a first component contained in at least one secret generated by at least one of the plurality of centers, the first component corresponding to one or more of the divided pieces of information specifying said another entity as recited in the independent claims of the present invention.

Although the Baba reference discusses a plurality of centers, the Baba reference does not allow for each of the centers to generate secret keys, such that a specific center does not have to have all of the secret keys. The divided information used to generate each of the secret keys at each of the centers allows for a diminished size of the secret key.

Further, Baba does not teach nor suggest that each entity generates a common key by using a component of the secret key corresponding to the divided information corresponding to another entity as recited in the claims of the present invention.

Thus, it is submitted that the independent claims are patentable over the cited reference. The dependent claims are also patentable over the cited reference,

Appl. No. 09/489,696  
Amdt. Dated July 12, 2004  
Reply to Office Action of February 12, 2004

Attorney Docket No. 81800.0018  
Customer No.: 26021

not only because they contain all of the limitations of the independent claims, but because the dependent claims also describe additional novel elements and features that are not described in the prior art.

### Conclusion

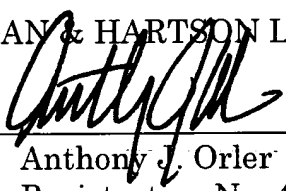
In view of the foregoing, it is respectfully submitted that the application is in condition for allowance. Reexamination and reconsideration of the application, as amended, are requested.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California telephone number (213) 337-6742 to discuss the steps necessary for placing the application in condition for allowance.

If there are any fees due in connection with the filing of this response, please charge the fees to our Deposit Account No. 50-1314.

Respectfully submitted,  
HOGAN & HARTSON L.L.P.

Date: July 12, 2004

By:   
Anthony J. Orler  
Registration No. 41,232  
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900  
Los Angeles, California 90071  
Phone: 213-337-6700  
Fax: 213-337-6701